The microprocessor 1138 also interacts with other device subsystems, such as the display 1122, Flash memory 1124, RAM 1126, auxiliary input/output (I/O) subsystems 1128, serial port 1130, keyboard 1132, speaker 1134, microphone 1136, a short-range communications subsystem 1140 and any other device subsystems generally designated as 1142.

Some of the subsystems shown in Fig. 11 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 1132 and display 1122 may be used for both communication-related functions, such as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

Operating system software used by the microprocessor 1138 is preferably stored in a persistent store such as Flash memory 1124. In addition to the operating system, which controls low-level functions of the mobile device 1110, the Flash memory 1124 may include a plurality of high-level software application programs, or modules, such as a voice communication module 1124A, a data communication module 1124B, an organizer module (not shown), or any other type of software module 1124N. These modules are executed by the microprocessor 1138 and provide a high-level interface between a user and the mobile device 100. This interface typically includes a graphical component provided through the display 1122, and an input/output component provided through the auxiliary I/O 1128, keyboard 1132, speaker 1134, and microphone 1136. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM 1126 for faster operation. Moreover, received communication signals may also be temporarily stored to RAM 1126, before

permanently writing them to a file system located in a persistent store such as the Flash memory 1124.

An exemplary application module 1124N that may be loaded onto the mobile device 100 is a personal information manager (PIM) application providing PDA functionality, such as calendar events, appointments, and task items. This module 1124N may also interact with the voice communication module 1124A for managing phone calls, voice mails, etc., and may also interact with the data communication module for managing e-mail communications and other data transmissions. Alternatively, all of the functionality of the voice communication module 1124A and the data communication module 1124B may be integrated into the PIM module.

The Flash memory 1124 preferably also provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 1124A, 1124B, via the wireless networks 1119. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless networks 1119, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

Decrypted session keys or other encryption accessing information is preferably stored on the mobile device 100 in a volatile and non-persistent store such as the RAM 1126. Such information may instead be stored in the Flash memory 1124, for example, when storage intervals are relatively short, such that the information is removed from memory soon after it is stored. However, storage of this information in the RAM 1126 or another volatile and non-persistent store is preferred, in order to ensure that the information is erased from memory when the mobile device 100 loses power. This prevents an unauthorized party from obtaining any

stored encryption accessing information such as a decrypted session key by removing a memory chip from the mobile device 100, for example.

The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 1130 of the mobile device 100 to the serial port of a computer system or device. The serial port 1130 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 1124N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 1119. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 1130. For example, a USB port would provide an interface to a similarly equipped personal computer.

Additional application modules 1124N may be loaded onto the mobile device 100 through the networks 1119, through an auxiliary I/O subsystem 1128, through the serial port 1130, through the short-range communications subsystem 1140, or through any other suitable subsystem 1142, and installed by a user in the Flash memory 1124 or RAM 1126. Such flexibility in application installation increases the functionality of the mobile device 100 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile device 100.

When the mobile device 100 is operating in a data communication mode, a received signal, such as a text message or a web page download, will be processed by the transceiver module 1111 and provided to the microprocessor 1138, which will preferably further process the received signal for output to the display 1122, or, alternatively, to an auxiliary I/O device 1128.

A user of mobile device 100 may also compose data items, such as e-mail messages, using the keyboard 1132, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 100 is further enhanced with a plurality of auxiliary I/O devices 1128, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user may then be transmitted over the communication networks 1119 via the transceiver module 1111.

When the mobile device 100 is operating in a voice communication mode, the overall operation of the mobile device is substantially similar to the data mode, except that received signals are preferably be output to the speaker 1134 and voice signals for transmission are generated by a microphone 1136. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the mobile device 100. Although voice or audio signal output is preferably accomplished primarily through the speaker 1134, the display 1122 may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information. For example, the microprocessor 1138, in conjunction with the voice communication module and the operating system software, may detect the caller identification information of an incoming voice call and display it on the display 1122.

A short-range communications subsystem 1140 may also be included in the mobile device 100. For example, the subsystem 1140 may include an infrared device and associated circuits and components, or a short-range RF communication module such as a Bluetooth™ module or an 802.11 module to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that "Bluetooth" and "802.11" refer to sets of

specifications, available from the Institute of Electrical and Electronics Engineers, relating to wireless personal area networks and wireless local area networks, respectively.

WHAT IS CLAIMED AS THE INVENTION IS:

1. A method for processing encrypted messages at a wireless mobile communication device, comprising the steps of:

receiving at the wireless mobile communication device an encrypted message comprising at least one encrypted session key and encrypted content;

accessing the encrypted message;

identifying an individual encrypted session key associated with the wireless mobile communication device;

decrypting the individual encrypted session key; and

storing the decrypted session key to memory;

wherein the stored decrypted session key is used to decrypt the encrypted content of the encrypted message where the encrypted content is subsequently accessed.

2. The method of claim 1, wherein the encrypted message is received by the wireless mobile communication device through a wireless infrastructure and a wireless network.

3. The method of claim 2, wherein a message server transmits the encrypted message through the wireless infrastructure and the wireless network to the wireless mobile communication device.

4. The method of claim 3, wherein the message server receives the encrypted message from a message sender.

5. The method of claim 4, wherein the wireless mobile communication device requests in a pull message access scheme that stored messages be forwarded by the message server to the wireless mobile communication device.

6. The method of claim 4, wherein the message server routes the encrypted message to the wireless mobile communication device when the encrypted message is received at the message server, and wherein the encrypted message is addressed by the message sender using a specific e-mail address associated with the wireless mobile communication device.

7. The method of claim 4, wherein the message server redirects the encrypted message to the wireless mobile communication device.

8. The method of claim 4, wherein the message server comprises means for redirecting the encrypted message to the wireless mobile communication device.

9. The method of claim 8, wherein, before the encrypted message is redirected to the wireless mobile communication device, a redirection program re-envelopes the encrypted message so as to maintain the addressing information of the encrypted message.

10. The method of claim 9, wherein the redirection program re-envelopes the encrypted message so as to allow a reply message generated by the wireless mobile communication device to reach the message sender.

11. The method of claim 1, further comprising, after the step of identifying, the steps of:

determining whether the encrypted session key has been decrypted and stored to the memory; and

retrieving the decrypted session key from the memory and using the stored decrypted session key to decrypt the encrypted content of the encrypted content where the encrypted session key has been decrypted and stored to the memory.

12. The method of claim 11, wherein the steps of decrypting and storing are performed where the encrypted session key has not been decrypted and stored to the memory.

13. The method of claim 1, wherein certificate information of a user of the wireless mobile communication device is transferred to the wireless mobile communication device through a wireless mobile communication device information transfer means.

14. The method of claim 13, wherein the wireless mobile communication device information transfer means comprises a wireless communication module.

15. The method of claim 14, wherein the wireless communication module is selected from the group consisting of: an infrared device, a Bluetooth module, and an 802.11 module.

16. The method of claim 1, wherein certificate revocation lists are transferred to the wireless mobile communication device through a wireless mobile communication device information transfer means.

17. The method of claim 16, wherein the wireless mobile communication device information transfer means comprises a serial port or a Universal Serial Bus (USB) port.

18. The method of claim 16, wherein the wireless mobile communication device information transfer means comprises an infrared device, a Bluetooth module, or an 802.11 module.

19. The method of claim 1, wherein the encrypted message is received by the wireless mobile communication device through means for providing a wireless infrastructure and through means for providing a wireless network.

20. The method of claim 19, wherein means for providing a message server transmits the encrypted message through the means for providing the wireless infrastructure to the wireless mobile communication device.

21. The method of claim 20, wherein the means for providing a message server receives the encrypted message from a message sender.

22. The method of claim 1, wherein a message server transmits the encrypted message through a wireless infrastructure and a wireless network to the wireless mobile communication device,

wherein the encrypted message comprises a plurality of encrypted session keys, wherein the message server determines the encrypted session key associated with the wireless mobile communication device, and wherein the message server reorganizes the encrypted message such that the encrypted message is sent to the wireless mobile communication device without containing at least one encrypted session key that is not associated with the wireless mobile communication device.

23. The method of claim 22, wherein the encrypted message comprises a digital signature, and wherein the message server verifies the digital signature and sends to the wireless mobile communication device a result of the digital signature verification.

24. The method of claim 1, wherein the encrypted message comprises a plurality of encrypted session keys, wherein the encrypted session keys are associated with different recipients, and wherein the encrypted message is reorganized prior to transmission to the wireless mobile communication device such that the encrypted message is transmitted to the wireless mobile communication device containing only the encrypted session key associated with the wireless mobile communication device.

25. The method of claim 24, wherein the encrypted message comprises a digital signature, and wherein the message server verifies the digital signature and sends to the wireless mobile communication device the result of the digital signature verification.

26. The method of claim 1, wherein the encrypted session key is a one-time session key that is generated and used for the encrypted message.

27. The method of claim 26, wherein the session key was encrypted using a public key associated with the wireless mobile communication device.

28. The method of claim 27, wherein the encrypted message was addressed to more than one receivers, and wherein the same session key is encrypted using a public key associated with each receiver.

29. The method of claim 1, wherein the encrypted content was encrypted using a session key and encryption algorithm, and wherein a public key cryptographic algorithm was used to encrypt the session key to generate the encrypted session key.

30. The method of claim 1, wherein the encrypted message was encrypted using Secure Multipurpose Internet Mail Extensions (S/MIME) techniques.

31. The method of claim 1, wherein the encrypted message was encrypted using Pretty Good Privacy techniques.

32. The method of claim 1, wherein the encrypted message was encrypted using OpenPGP techniques.

33. The method of claim 1, wherein the encrypted message comprises a digital signature.

34. The method of claim 1, wherein the encrypted message comprises an e-mail message.

35. The method of claim 1, wherein the decrypted session key is removed from the memory after a preselected time has elapsed.

36. The method of claim 35, wherein the preselected time is selected by the user.

37. The method of claim 1, wherein the decrypted session key is removed from the memory based upon a characteristic associated with the encrypted message.

38. The method of claim 37, wherein the decrypted session key is removed from the memory based upon electrical power being removed from the wireless mobile communication device.

39. The method of claim 37, wherein the characteristic comprises the identity of a sender of the encrypted message.

40. The method of claim 39, wherein the identity of the sender of the encrypted message comprises an e-mail address of the sender.

41. The method of claim 1, wherein the decrypted session key is removed from the memory based upon a sensitivity level of the encrypted message.

42. The method of claim 41, wherein the sensitivity level is determined based upon a subject line contained within the encrypted message.

43. The method of claim 41, wherein the sensitivity level is determined based upon the encrypted content.

44. The method of claim 1, further comprising the step of:

setting a disabling flag so that the decrypted session key is not continuously stored in the memory for use in additional accesses of the encrypted content.

45. The method of claim 1, further comprising the step of:

setting a disabling flag so that the decrypted session key is removed from the memory after accessing the encrypted content.

46. The method of claim 1, wherein the decrypted session key is stored to a volatile memory of the wireless mobile communication device.

47. The method of claim 1, wherein the decrypted session key is stored to a volatile and non-persistent memory of the wireless mobile communication device.

48. The method of claim 1, wherein the decrypted session key is stored to a random access memory (RAM) of the wireless mobile communication device.

49. The method of claim 1, wherein a user of the wireless mobile communication device enters security information in order to have the encrypted session key decrypted.

50. The method of claim 49, wherein the security information comprises a password.

51. An apparatus for processing encrypted messages at a wireless mobile communication device, comprising:

means for receiving an encrypted message comprising at least one encrypted session key and encrypted content;

means for accessing the encrypted message;

means for identifying an individual encrypted session key associated with the wireless mobile communication device where the encrypted message is accessed by the means for accessing;

means for decrypting the individual encrypted session key; and

means for storing the decrypted session key to memory;

wherein the stored decrypted session key is used to decrypt the encrypted content of the encrypted message where the encrypted content is subsequently accessed by the means for accessing.

52. Computer software stored on a computer readable medium, the computer software comprising program code for carrying out a method that processes an encrypted message at a wireless mobile communication device when the encrypted message is accessed, said encrypted

message containing at least one encrypted session key and encrypted content, said method comprising the steps of:

identifying an individual encrypted session key associated with the wireless mobile communication device where the encrypted message is accessed by the means for accessing;

decrypting the individual encrypted session key;

storing the decrypted session key to memory; and

using the stored decrypted session key to decrypt the encrypted content where the encrypted content is accessed multiple times.

53. An apparatus on a wireless mobile communication device for handling multiple accesses to encrypted content, wherein an encrypted message includes the encrypted content and further includes encryption accessing information, and wherein the encrypted message is transmitted to the wireless mobile communication device, the apparatus comprising:

a storage software module that stores the encryption accessing information in memory which is volatile and non-persistent, wherein the encryption accessing information allows access to the encrypted content; and

an accessing software module that retrieves from the memory the encryption accessing information,

wherein the retrieved encryption accessing information is used to decrypt the encrypted content where the encrypted content is accessed multiple times.

54. The apparatus of claim 53, wherein the encryption accessing information comprises a session key.

55. The apparatus of claim 53, wherein the encrypted message further comprises a digital signature, wherein the storage software module stores, in the memory, verification information about the digital signature, and wherein the software accessing module retrieves from the memory the verification information when the encrypted content is accessed multiple times.

56. The apparatus of claim 55, further comprising a data structure stored in the memory for containing the verification information and the encryption accessing information.

57. The apparatus of claim 56, wherein the wireless mobile communication device receives a plurality of encrypted messages, and wherein the data structure associates which encryption accessing information is associated with which message.

58. The apparatus of claim 57, wherein the data structure associates which verification information is associated with which message.

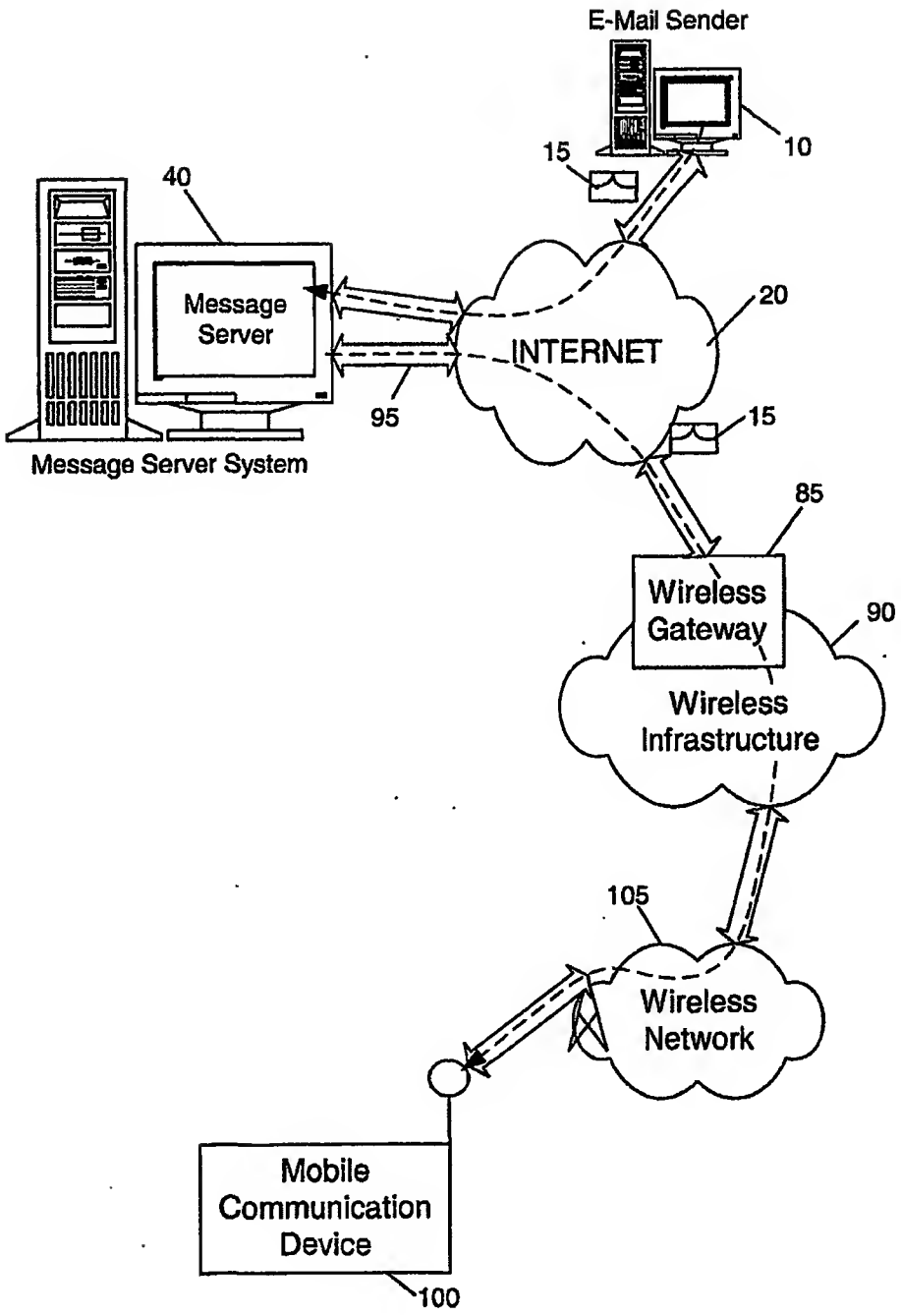
E-Mail Sender
10
15
40
Message Server
Message Server System
95
INTERNET
20
15
85
Wireless Gateway
90
Wireless Infrastructure
105
Wireless Network
Mobile Communication Device
100

FIG. 1

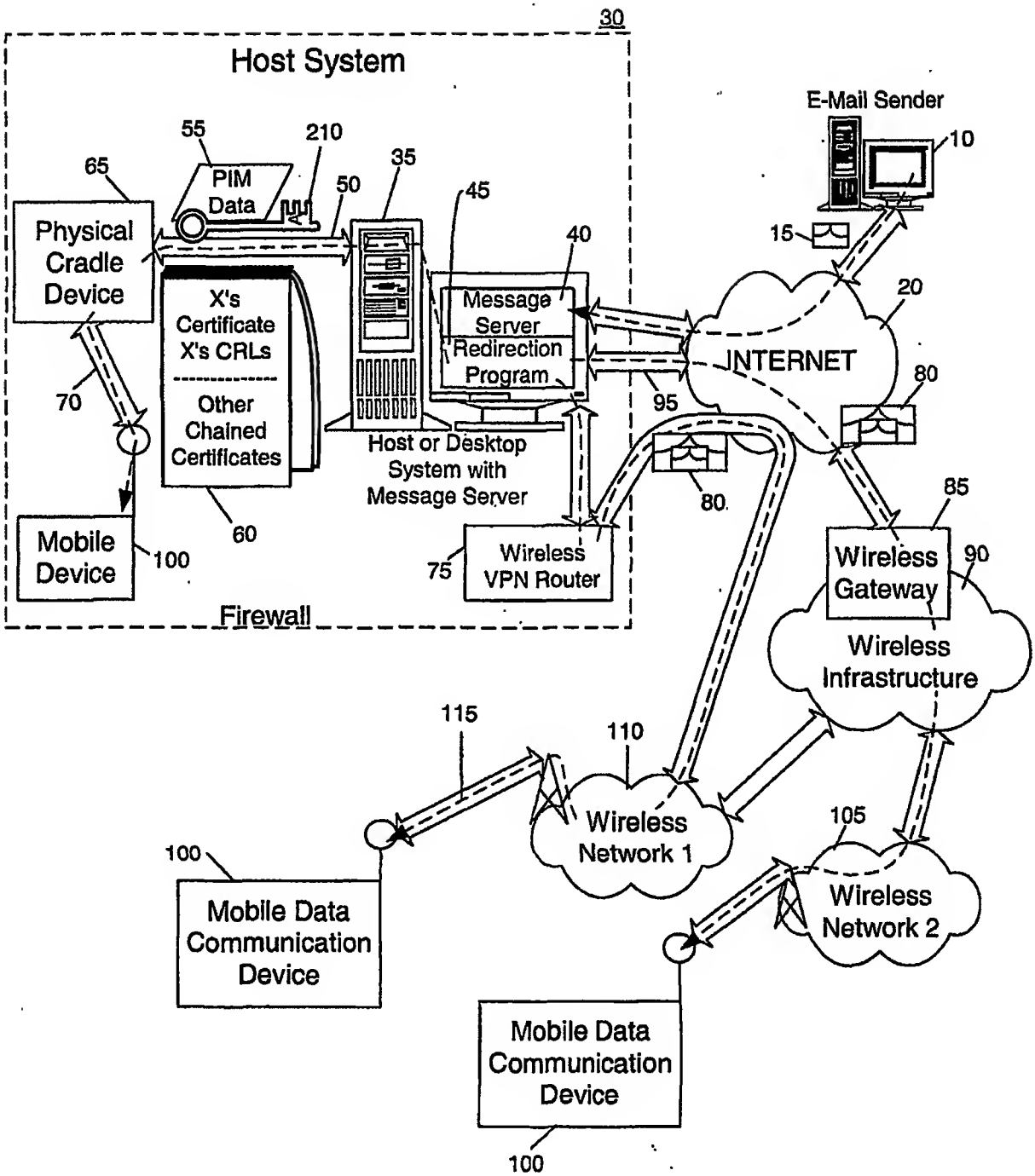
30
Host System
55
210
35
65
PIM Data
50
45
40
Physical Cradle Device
X's Certificate
X's CRLs
Other Chained Certificates
Message Server
Redirection Program
Host or Desktop System with Message Server
70
60
95
Mobile Device
100
75
Wireless VPN Router
Firewall
E-Mail Sender
10
15
20
INTERNET
80
80
85
Wireless Gateway
90
Wireless Infrastructure
115
110
Wireless Network 1
105
Wireless Network 2
100
Mobile Data Communication Device
Mobile Data Communication Device
100

FIG. 2

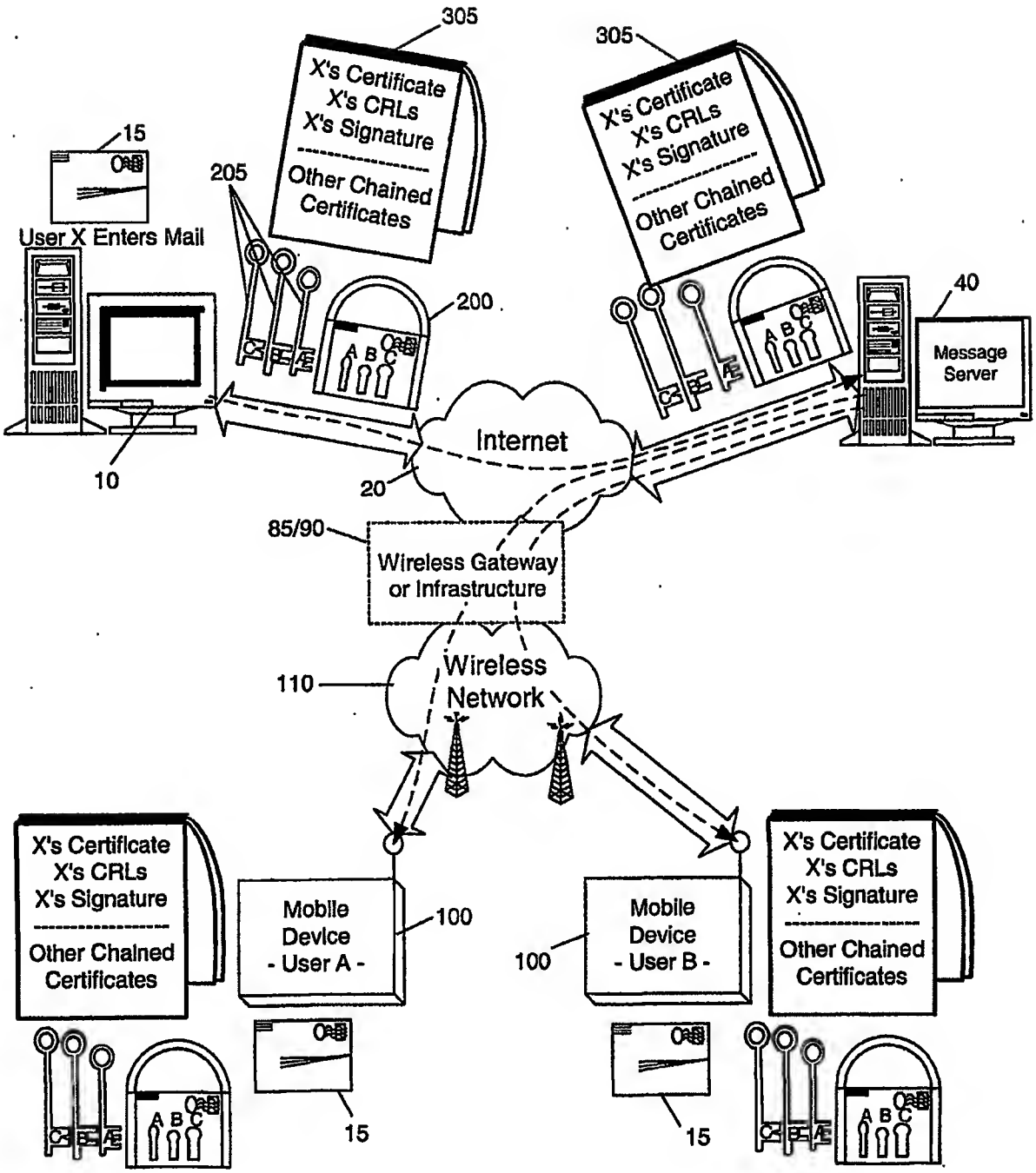
305
X's Certificate
X's CRLs
X's Signature
Other Chained Certificates
305
X's Certificate
X's CRLs
X's Signature
Other Chained Certificates
15
User X Enters Mail
205
200
40
Message Server
10
Internet
20
85/90
Wireless Gateway or Infrastructure
110
Wireless Network
X's Certificate
X's CRLs
X's Signature
Other Chained Certificates
Mobile Device - User A -
100
Mobile Device - User B -
100
X's Certificate
X's CRLs
X's Signature
Other Chained Certificates
15
15

FIG. 3

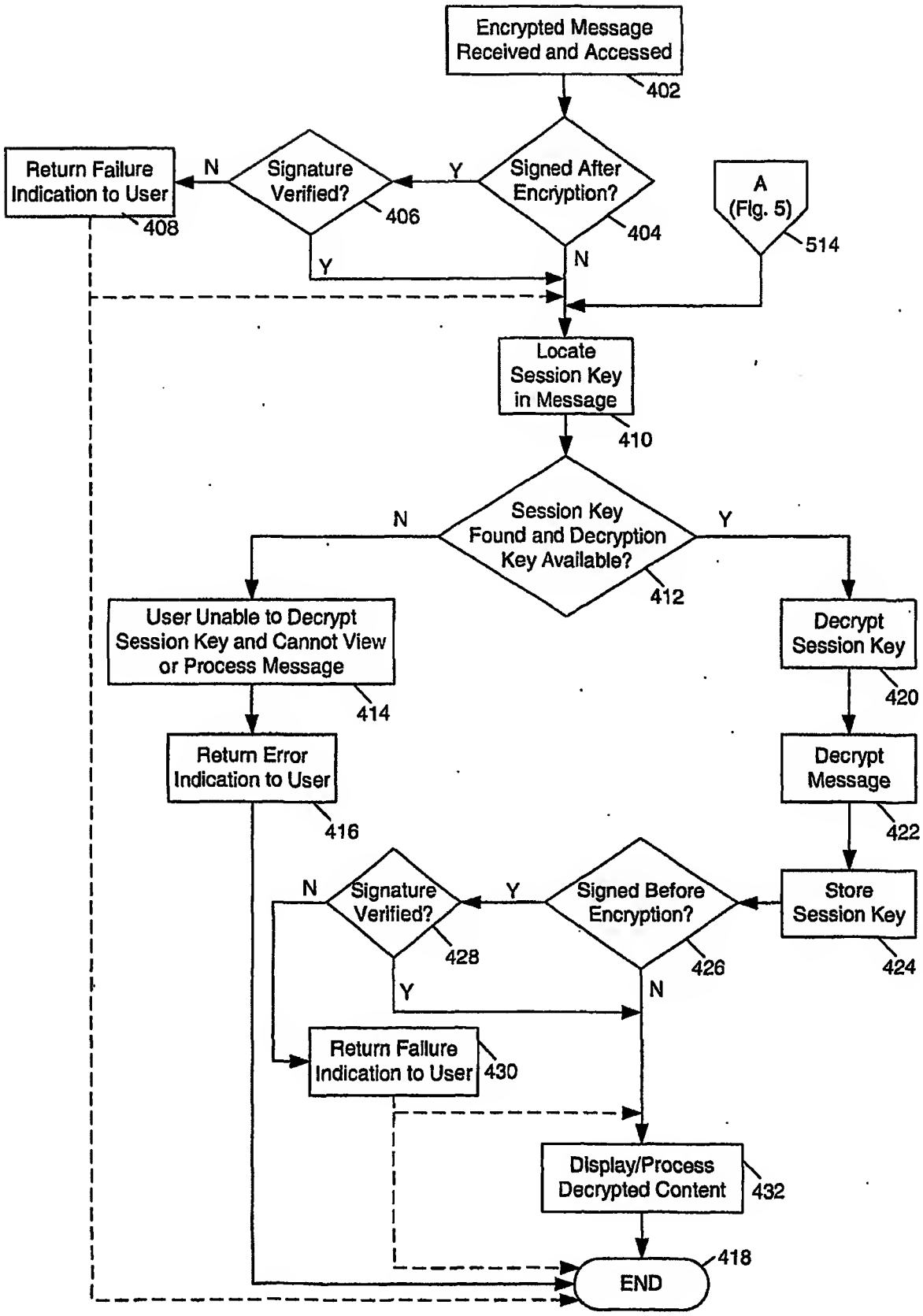
Encrypted Message Received and Accessed
402
Signed After Encryption?
404
Y
N
Signature Verified?
406
Y
N
Return Failure Indication to User
408
A (Fig. 5)
514
Locate Session Key in Message
410
Session Key Found and Decryption Key Available?
412
N
Y
User Unable to Decrypt Session Key and Cannot View or Process Message
414
Return Error Indication to User
416
Decrypt Session Key
420
Decrypt Message
422
Store Session Key
424
Signed Before Encryption?
426
Y
N
Signature Verified?
428
N
Y
Return Failure Indication to User
430
Display/Process Decrypted Content
432
END
418

FIG. 4

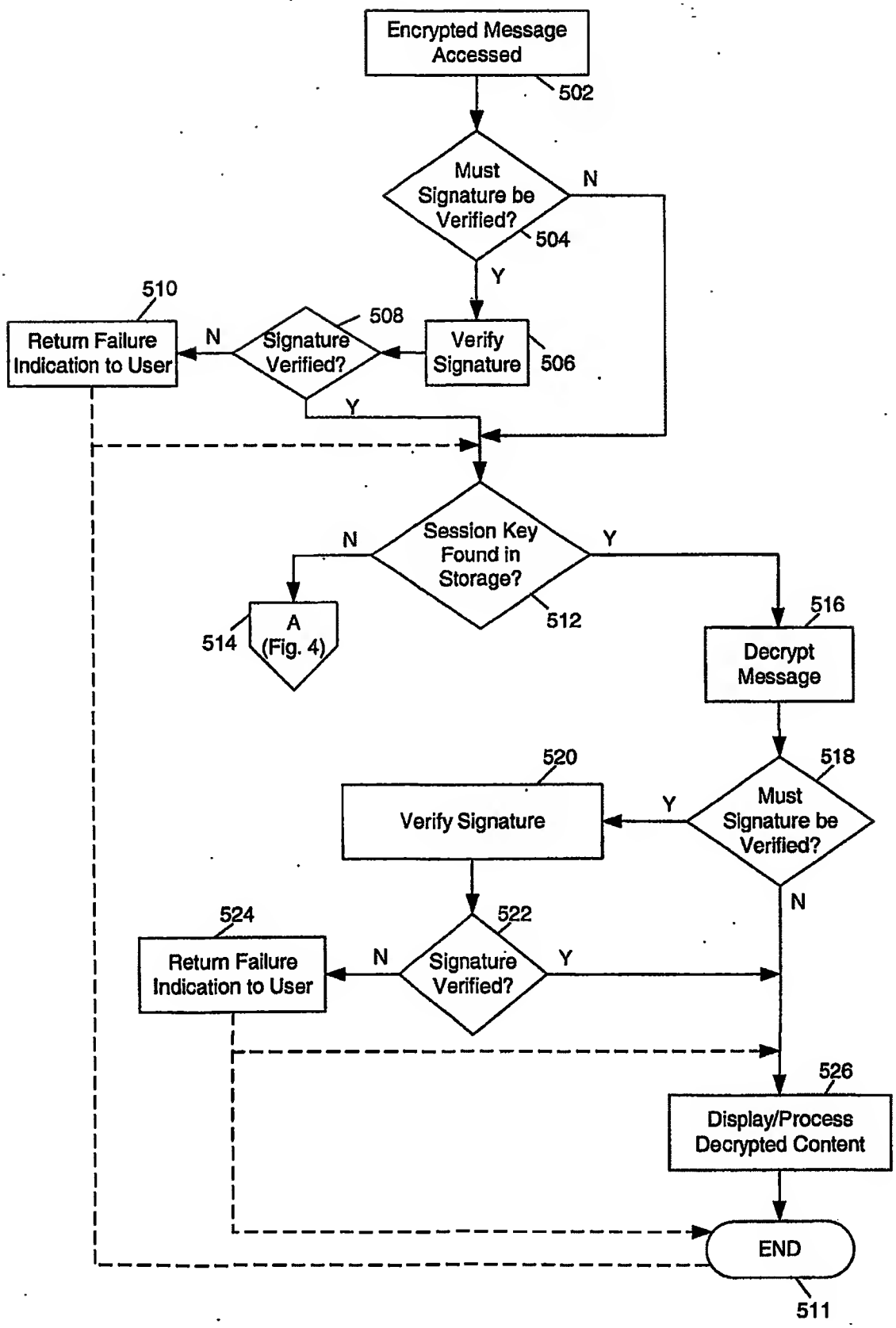
Encrypted Message Accessed
502
Must Signature be Verified?
504
N
Y
Verify Signature
506
Signature Verified?
508
N
Y
Return Failure Indication to User
510
Session Key Found in Storage?
512
N
Y
A (Fig. 4)
514
Decrypt Message
516
Must Signature be Verified?
518
Y
N
Verify Signature
520
Signature Verified?
522
N
Y
Return Failure Indication to User
524
Display/Process Decrypted Content
526
END
511

FIG. 5

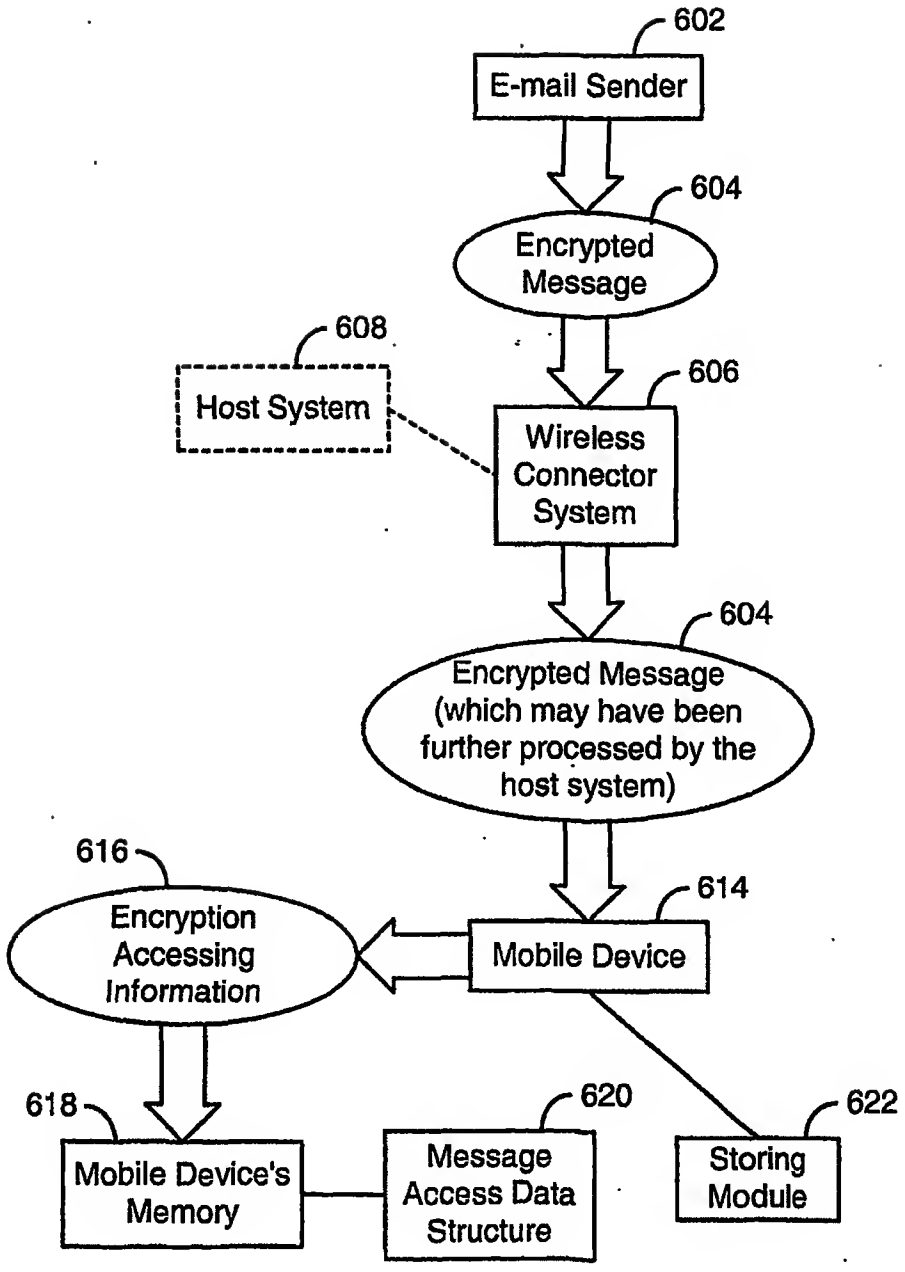
602
E-mail Sender
604
Encrypted Message
608
Host System
606
Wireless Connector System
604
Encrypted Message (which may have been further processed by the host system)
616
Encryption Accessing Information
614
Mobile Device
618
Mobile Device's Memory
620
Message Access Data Structure
622
Storing Module

FIG. 6

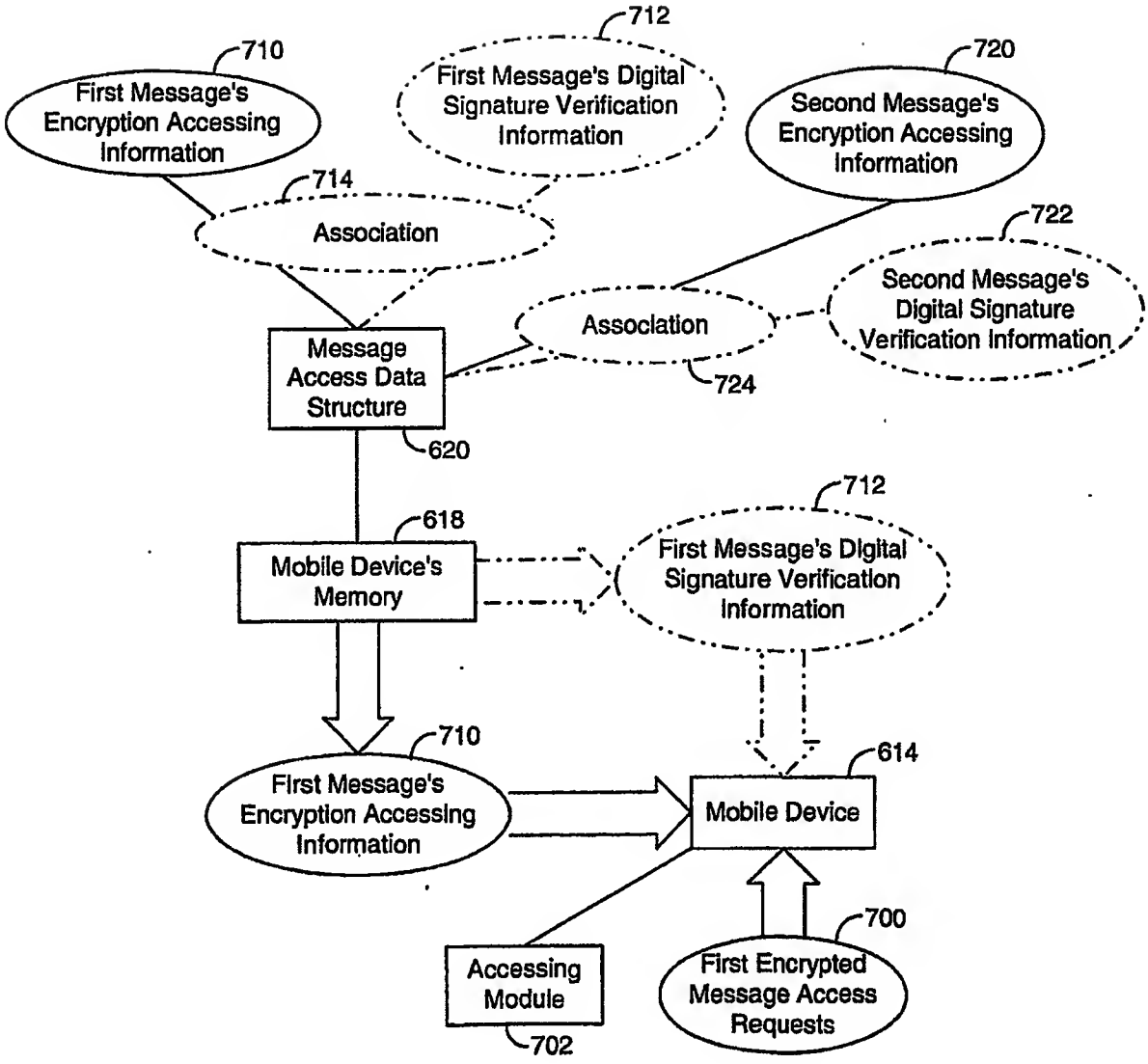
710
First Message's Encryption Accessing Information
712
First Message's Digital Signature Verification Information
720
Second Message's Encryption Accessing Information
714
Association
722
Second Message's Digital Signature Verification Information
Association
724
Message Access Data Structure
620
618
Mobile Device's Memory
712
First Message's Digital Signature Verification Information
710
First Message's Encryption Accessing Information
614
Mobile Device
700
First Encrypted Message Access Requests
Accessing Module
702

FIG. 7

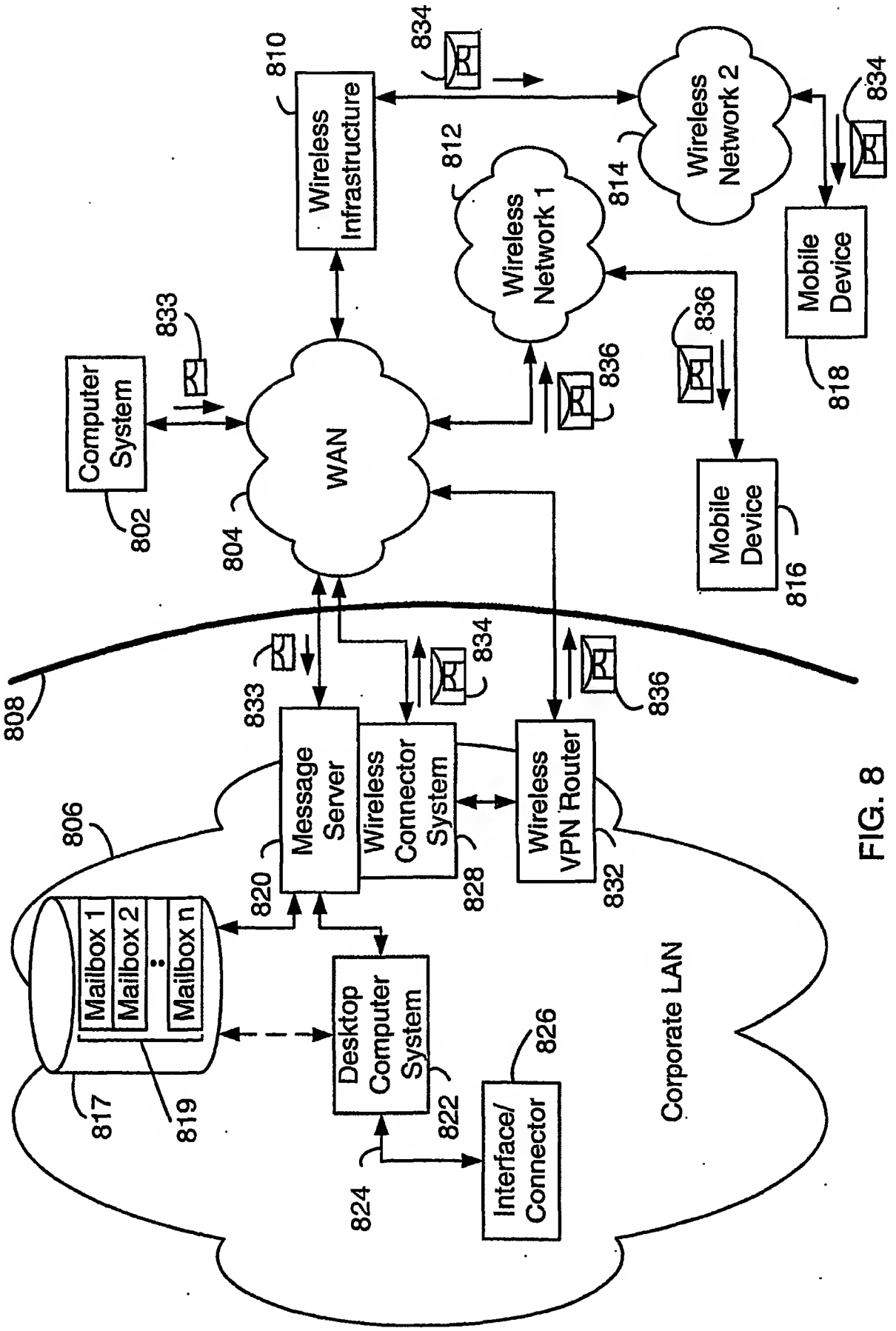
Wireless Infrastructure
810
834
Wireless Network 2
814
834
Wireless Network 1
812
Mobile Device
818
836
833
Computer System
802
WAN
804
836
Mobile Device
816
808
833
834
836
Message Server
820
Wireless Connector System
828
Wireless VPN Router
832
806
Mailbox 1
Mailbox 2
Mailbox n
817
819
Desktop Computer System
822
824
Interface/ Connector
826
Corporate LAN

FIG. 8

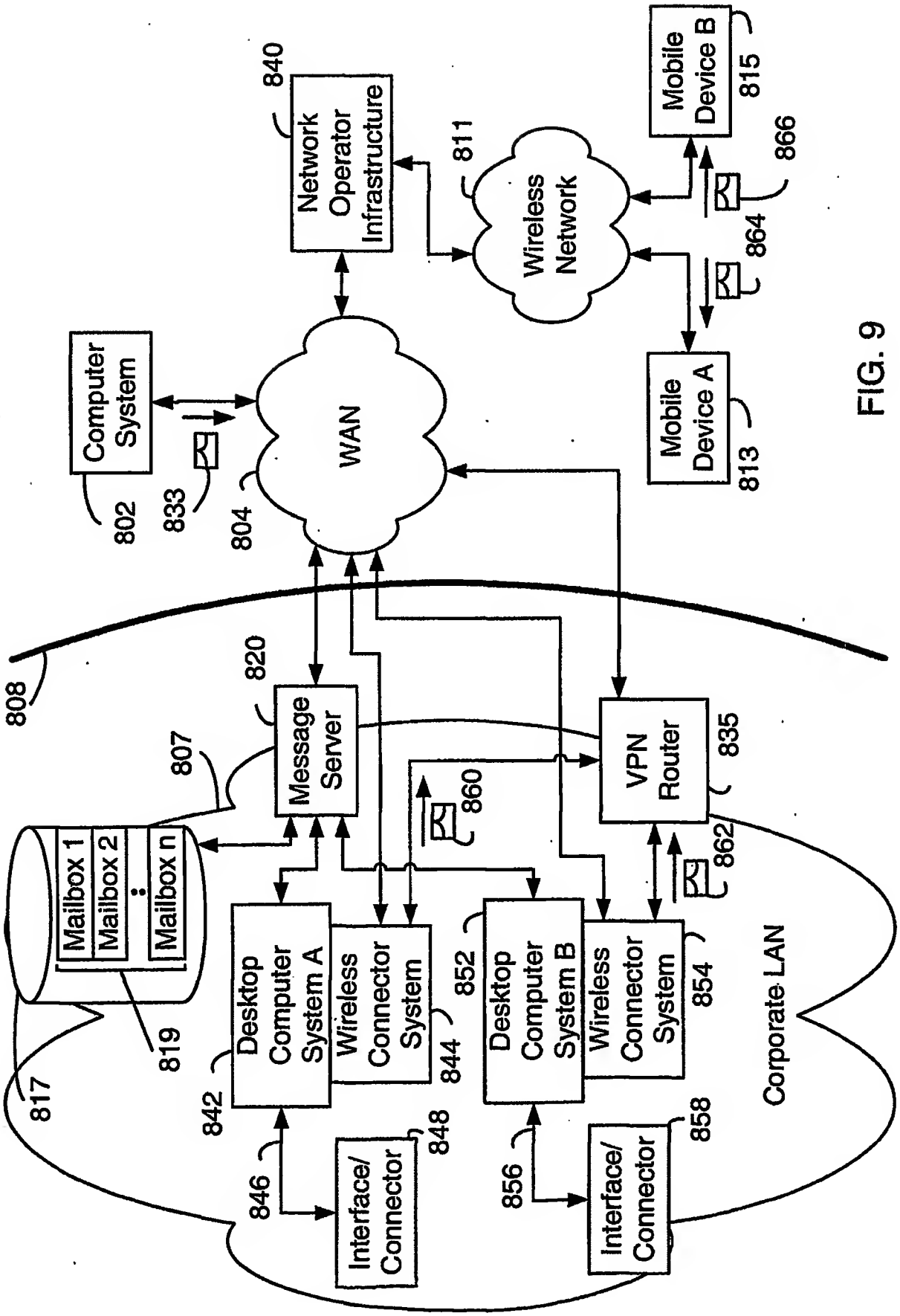
Corporate LAN
808
WAN
804
Network Operator Infrastructure
840
Wireless Network
811
Computer System
802
833
Mobile Device A
813
Mobile Device B
815
864
866
Message Server
820
807
VPN Router
835
860
862
Mailbox 1
Mailbox 2
Mailbox n
819
817
Desktop Computer System A
842
Wireless Connector System
844
Desktop Computer System B
852
Wireless Connector System
854
Interface/ Connector
846
848
Interface/ Connector
856
858

FIG. 9

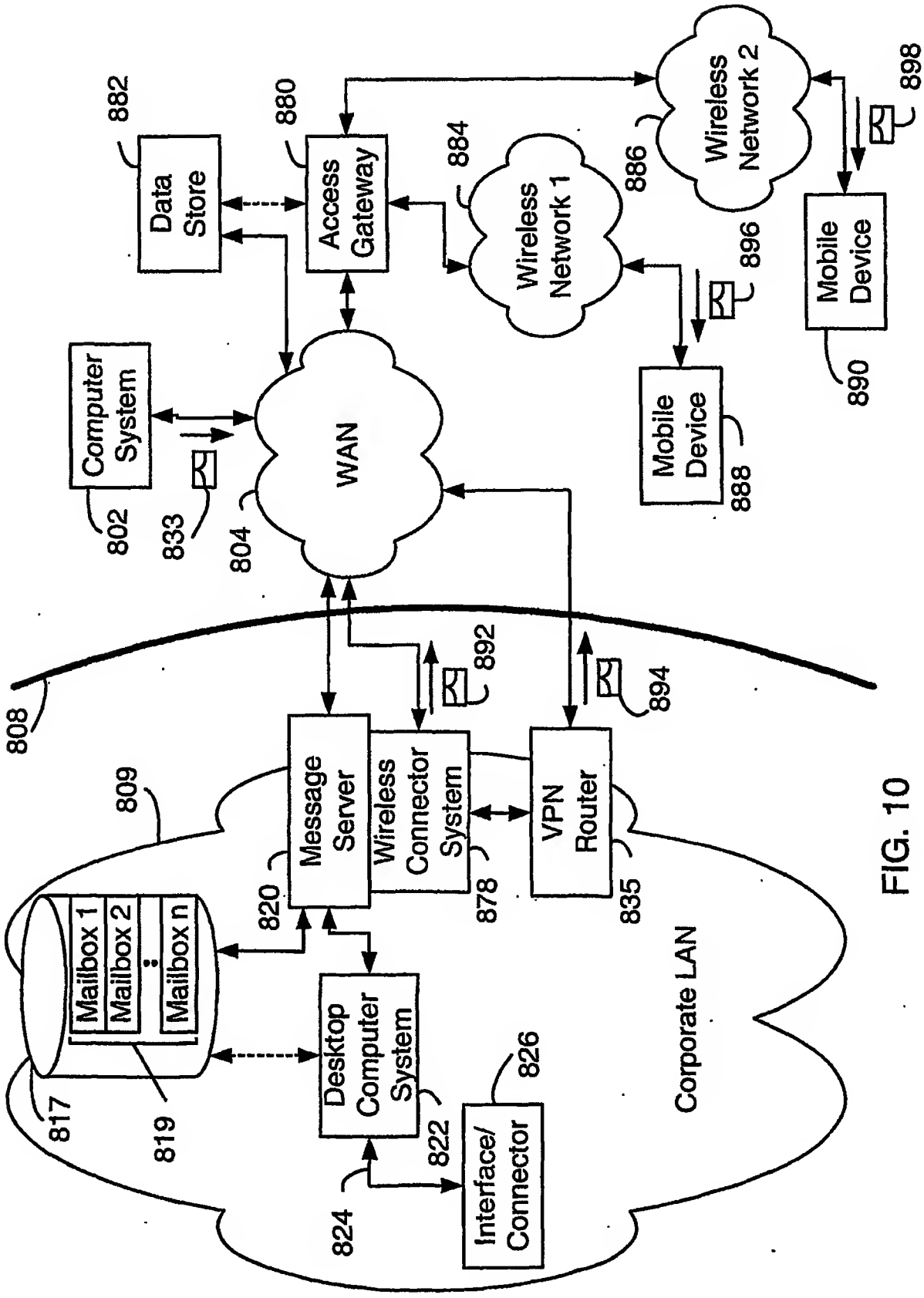
Data Store
882
Access Gateway
880
Wireless Network 1
884
Wireless Network 2
886
898
Mobile Device
896
890
Computer System
802
833
WAN
804
Mobile Device
888
808
892
894
Message Server
820
Wireless Connector System
878
VPN Router
835
809
Mailbox 1
Mailbox 2
Mailbox n
817
819
Desktop Computer System
822
824
826
Interface/ Connector
Corporate LAN

FIG. 10

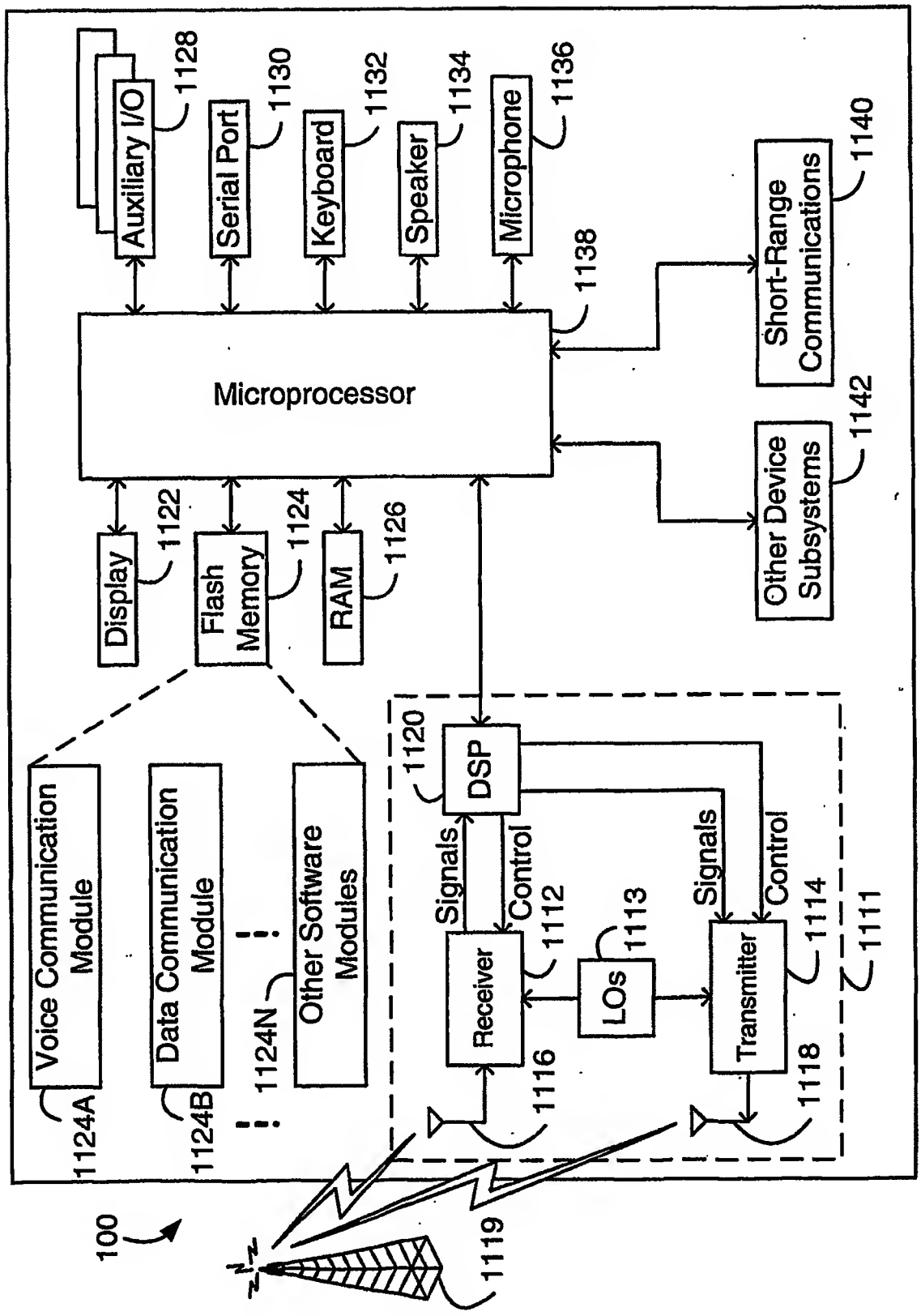
100
1119
1124A
Voice Communication Module
1124B
Data Communication Module
1124N
Other Software Modules
Display
1122
Flash Memory
1124
RAM
1126
Microprocessor
1138
Auxiliary I/O
1128
Serial Port
1130
Keyboard
1132
Speaker
1134
Microphone
1136
Short-Range Communications
1140
Other Device Subsystems
1142
1120
DSP
Signals
Control
1112
Receiver
1116
LOs
1113
Signals
Control
1114
Transmitter
1118
1111

FIG. 11

INTERNATIONAL SEARCH REPORT

Application No
PCT/CA 02/01060

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 229 894 B1 (VAN OORSCHOT PAUL C ET AL) 8 May 2001 (2001-05-08)	1,13,29, 33,34, 51-54
Y		2-16, 19-21, 26, 30-32, 35,36, 39,40, 44-50
A		17, 22-25, 27,28, 37,38, 55-58
	column 1, line 11-51 column 3, line 33 -column 6, line 63 figure 2	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 November 2002	26/11/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kopp, K

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 096 725 A (RES IN MOTION LTD) 2 May 2001 (2001-05-02)	2-14, 19-21
A	paragraphs '0001!,'0002! paragraphs '0009!-'0012! paragraphs '0014!,'0015! paragraphs '0020!,'0021! paragraphs '0025!-'0028! paragraphs '0032!,'0033! paragraphs '0036!,'0037! paragraph '0047! figures 1,2	22
Y	WO 00 72506 A (IBM UK ;IBM (US)) 30 November 2000 (2000-11-30) page 1, line 22 -page 2, line 14	14,15, 35,36
A	page 2, line 37 -page 4, line 4 page 5, line 9 -page 6, line 8 page 8, line 14-25 page 10, line 15 -page 12, line 2 page 14, line 29 -page 15, line 22	18
Y	DATABASE IETF RFC 'Online! IETF; RFC 2312 S/MIME Version 2 certificate Handling, March 1998 (1998-03) S. DUSS ET AL: "S/MIME Version 2 Certificate Handling" retrieved from HTTP://WWW.IETF.ORG XP002220385 Chapter 2.1 Chapter 4.1	16
A	WO 99 27678 A (NOKIA TELECOMMUNICATIONS OY ;LEIWO JUSSIPEKKA (FI)) 3 June 1999 (1999-06-03) page 3, line 22-30 page 4, line 3 -page 5, line 15 page 8, line 16-20 page 9, line 1-8	23,25
Y	US 6 073 237 A (ELLISON CARL) 6 June 2000 (2000-06-06) column 1, line 56 -column 4, line 39 column 5, line 1-17	26

-/--

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	BROWN M ET AL: "PGP in Constrained Wireless Devices" PROCEEDINGS OF THE USENIX SECURITY SYMPOSIUM, XX, XX, 14 August 2000 (2000-08-14), pages 247-261, XP002210575 Chapter 1 Chapter 2 Chapter 3 Chapter 4 ---	30-32, 39,40, 49,50
Y	WO 96 36934 A (SMART TOUCH L L C) 21 November 1996 (1996-11-21) page 25, line 14 -page 26, line 28 page 27, line 29-33 page 40, line 7-10 page 47, line 21-24 page 56, line 13-19 page 151, line 13 -page 153, line 15 ---	44-48
A	DATABASE IETF RFC 'Online! IETF; RFC 2634, June 1999 (1999-06) HOFFMAN: "Enhanced Services for S/MIME" XP002220386 Chapter 3, Security Labels page 24 -page 32 -----	41-43

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 02/01060

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 6229894	B1	08-05-2001	NONE		
EP 1096725	A	02-05-2001	US	6219694 B1	17-04-2001
			EP	1096725 A2	02-05-2001
			EP	1096726 A2	02-05-2001
			EP	1096727 A2	02-05-2001
			EP	1098481 A2	09-05-2001
			EP	1124352 A2	16-08-2001
			EP	1126662 A2	22-08-2001
			EP	1206073 A2	15-05-2002
			AU	3924499 A	20-12-1999
			CA	2333881 A1	09-12-1999
			WO	9963709 A2	09-12-1999
			CN	1304608 T	18-07-2001
			EP	1082839 A2	14-03-2001
			JP	2002517947 T	18-06-2002
			NO	20005917 A	26-01-2001
			US	6463464 B1	08-10-2002
			US	6463463 B1	08-10-2002
			US	2001009015 A1	19-07-2001
			US	2001013071 A1	09-08-2001
			US	2001005860 A1	28-06-2001
			US	2001004744 A1	21-06-2001
			US	2001005861 A1	28-06-2001
			US	2001005857 A1	28-06-2001
			US	2002120696 A1	29-08-2002
			US	2001054115 A1	20-12-2001
			US	2002029258 A1	07-03-2002
			US	2002049818 A1	25-04-2002
WO 0072506	A	30-11-2000	AU	5084500 A	12-12-2000
			CN	1351789 T	29-05-2002
			CZ	20014168 A3	15-05-2002
			EP	1179244 A1	13-02-2002
			WO	0072506 A1	30-11-2000
			HU	0201561 A2	28-09-2002
WO 9927678	A	03-06-1999	FI	974341 A	27-05-1999
			AU	1240499 A	15-06-1999
			CA	2310329 A1	03-06-1999
			CN	1280727 T	17-01-2001
			EP	1025675 A2	09-08-2000
			WO	9927678 A2	03-06-1999
			JP	2001524777 T	04-12-2001
US 6073237	A	06-06-2000	AU	1901099 A	31-05-1999
			WO	9924895 A1	20-05-1999
WO 9636934	A	21-11-1996	US	5613012 A	18-03-1997
			AU	5922696 A	29-11-1996
			BR	9608580 A	05-01-1999
			CA	2221321 A1	21-11-1996
			CN	1191027 A	19-08-1998
			EP	0912959 A1	06-05-1999
			JP	11511882 T	12-10-1999
			WO	9636934 A1	21-11-1996
			US	2002111917 A1	15-08-2002
			US	6366682 B1	02-04-2002

INTERNATIONAL SEARCH REPORT

Information on patent family members

Application No
PCT/CA 02/01060

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9636934 A		US 6269348 B1	31-07-2001
		US 6230148 B1	08-05-2001
		US 6192142 B1	20-02-2001
		US 6012039 A	04-01-2000
		US 6154879 A	28-11-2000
		US 6397198 B1	28-05-2002
		US 5838812 A	17-11-1998
		US 5870723 A	09-02-1999
		US 5764789 A	09-06-1998
		US 2001000535 A1	26-04-2001
		US 5802199 A	01-09-1998
		US 5805719 A	08-09-1998
		US 2001029493 A1	11-10-2001
		US 2001039533 A1	08-11-2001